In the claims:

For the Examiner's convenience, all pending claims are presented below with changes shown.

1. (Currently Amended) A portable device, which includes:

a wireless communication module to communicate with each of a plurality of remote devices within a locality;

a data storage module having a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner; and

a controller connected to the wireless communication module and to the data storage module, to ~~control~~ to establish a wireless communication link ~~of data~~ between the wireless communication module and a first remote device ~~by determining~~ based upon access rights associated with the first remote device to the public storage area and the private storage area.

2. (Canceled)

3. (Previously Presented) A portable device as claimed in Claim 1, in which the controller filters requests from each of the remote devices to exchange data and to reject and accept the requests in response to the nature of services offered by the remote device.

4. (Original) A portable device as claimed in Claim 1, in which the controller defines access rights to the first and second storage areas and, dependent upon the access rights,

allows the remote device to store and retrieve data from at least one of the first and second storage areas.

5. (Previously Presented) A portable device as claimed in Claim 1, in which a digital certificate of authenticity is requested from the remote device prior to communicating data between the remote device and the private storage area.

6. (Previously Presented) A portable device as claimed in Claim 1, in which the controller restricts how often and the amount of data which is writable by the remote device into the public storage area.

7. (Previously Presented) A portable device as claimed in Claim 1, in which data stored in the public storage area is selectively cleared by the controller in an automated fashion.

8. (Original) A portable device as claimed in Claim 1, in which the portable device and the remote device communicate using secure sockets layer (SSL) protocols.

9. (Original) A portable device as claimed in Claim 1, which detects Universal Plug and Play (UPnP) broadcasts.

10. (Original) A portable device as claimed in Claim 1, in which the wireless communication module is a radio frequency (RF) transceiver which communicates using a standardized communication protocol.

11. (Original) A portable device as claimed in Claim 10, in which the standardized communication protocol is selected from the group including Bluetooth IEEE 802.15 technology, IEEE 802.11a technology, and IEEE 802.11b technology.

12. (Previously Presented) A portable device as claimed in Claim 1, in which the controller interfaces the portable device to a computer system to permit a user to access and store data in the data storage module.

13. (Original) A device as claimed in Claim 1, in which the remote device is defined by another portable device within the locality.

14. (Original) A device as claimed in Claim 1, which includes a rechargeable power supply for powering its various components.

15. (Currently Amended) A data communication system, which includes:

a plurality of remote devices, each remote device including a wireless communication interface; and

at least one portable device, which includes:

a wireless communication module to communicate within a locality with the wireless communication interface the remote devices;

a data storage module having a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner; and

a controller connected to the wireless communication module and to the data storage module, to ~~control~~ to establish a wireless communication link ~~of data~~ between the wireless communication module and a first remote device ~~by determining~~ based upon access rights associated with the first remote device to the public storage area and the private storage area.

16. (Canceled)

17. (Original) A system as claimed in Claim 15, in which the controller filters requests from each of the remote devices to exchange data and to selectively reject and accept the requests in response to the nature of services offered by the remote device.

18. (Previously Presented) A system as claimed in Claim 15, in which the controller defines access rights to the first and second storage areas and, dependent upon the access rights, allows the remote device to store and retrieve data from at least one of the first and second storage areas.

19. (Previously Presented) A system as claimed in Claim 15, in which a digital certificate of authenticity is requested from the remote device prior to communicating data between the remote device and the private storage area.

20. (Previously Presented) A system as claimed in Claim 15, in which the controller restricts the amount of data which is writable by the remote device into the public storage area.

21. (Currently Amended) A method which includes:

monitoring, by means of a portable device, wireless communications from a plurality of remote devices requesting communications with the portable device within a locality, the portable device including a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner;

identifying access rights associated with the remote device; and

~~controlling the communication of data between the the remote device and the private and public storage areas dependent upon the access rights to the private and public storage areas~~

establishing a wireless communication link between the wireless communication module and a first remote device based upon access rights associated with the first remote device to the public storage area and the private storage area.

22. (Original) A method as claimed in Claim 21, which includes exchanging data in a relatively free manner between the first storage area, which defines a public data storage area, and the remote device, and exchanging data in a relatively restricted manner between the second storage area, which defines a private data storage area, and the remote device.

23. (Original) A method as claimed in Claim 21, which includes:

filtering requests for substantive communications from each of the remote devices with the portable device ; and

selectively rejecting and accepting the requests in response to the nature of services offered by the remote device.

24. (Original) A method as claimed in Claim 22, which includes defining access rights to the first and second storage areas and, dependent upon the access rights, allowing the remote device to store and retrieve data from at least one of the first and second storage areas.

25. (Original) A method as claimed in Claim 24, in which the access rights are dependent upon a classification of the remote device by the portable device.

26. (Original) A method as claimed in Claim 22, which includes requesting a digital certificate of authenticity from the remote device prior to communicating data between the remote device and the private storage area.

27. (Original) A method as claimed in Claim 22, which includes restricting the amount of data which is writable by the remote devices into the public storage area.

28. (Original) A method as claimed in Claim 22, which includes selectively clearing data in the public storage area.

29. (Original) A method as claimed in Claim 21, which includes communicating between the portable device and the remote device using secure sockets layer (SSL) protocols.

30. (Original) A method as claimed in Claim 21, which includes detecting universal plug and play (UPnP) broadcasts from each remote device.

31. (Original) A method as claimed in Claim 21, which includes communicating via a radio frequency (RF) transceiver using a standardized communication protocol.

32. (Original) A method as claimed in Claim 31, which includes communicating using technology selected from the group including Bluetooth 802.15 technology, IEEE 802.11a technology and IEEE 802.11b technology.

33. (Currently Amended) A computer program product including a medium readable by a computer, the medium carrying instructions which, when executed by the computer, cause the computer to:

monitor wireless communications within a locality from a plurality of remote devices requesting substantive communications with a portable device including the processor and a data storage module a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner;

identify access rights associated with the remote device; and

~~control the communication of data between the the remote device and the private and public storage areas dependent upon the access rights to the private and public storage areas~~

establish a wireless communication link between the wireless communication module and a first remote device based upon access rights associated with the first remote device to the public storage area and the private storage area.

34. (Original) A computer program product as claimed in Claim 33, in which data is exchanged in a relatively free manner between the first storage area, which defines a public data storage area, and the remote device, and data is exchanged in a relatively restricted manner between the second storage area, which defines a private data storage area, and the remote device.

35. (Original) A computer product as claimed in Claim 33, in which requests for substantive communications from each of the remote devices with the portable device are filtered, the requests being selectively rejected and accepted in response to the nature of services offered by the remote device.

36. (Original) A computer program product as claimed in Claim 33, which includes defining access rights to the first and second storage areas and, dependent upon the access rights, allowing the remote device to store and retrieve data from at least one of the first and second storage areas.

37. (Original) A computer program product as claimed in Claim 36, in which the access rights are dependent upon the classification of the remote device by the portable device.

38. (Original) A computer program product as claimed in Claim 34, which includes requesting a digital certificate of authenticity from the remote device prior to communicating data between the remote device and the private storage area.

39. (Original) A computer program product as claimed in Claim 34, which includes restricting how often and the amount of data which is writable by the remote devices into the public storage area.

40. (Original) A computer program product as claimed in Claim 34, which includes selectively clearing data in the public area.

41. (Original) A computer program product as claimed in Claim 33, which includes communicating between the portable device and the remote device using secure sockets layer (SSL) protocols.

42. (Original) A computer program product as claimed in Claim 33, which includes detecting universal plug and play (UPnP) broadcasts from each remote device.